An Effective Diffie-Hellman Key Based Intrusion Detection to Secure for Multicast Routing in MANET

M. Dhivyasri[1], P.E. Prem[2], A. Nithyasri[3]

[1]*(PG scholar, Department of Information Technology, VCEW)*

[2]*(Assistant Professor, Department of Information Technology, VCEW)*

3(Assistant Professor, Department of Information Technology, VCEW)

ABSTRACT- *An ad hoc mobile network is a collection of mobile nodes that are dynamically and arbitrarily located in such a manner that the interconnections between nodes are capable of changing on a continual basis. In order to facilitate communication within the network, a routing protocol is used to discover routes between nodes. In our network to using a movable nodes from one place to another, that time the attacker to hack the data on network. The Diffie-Hellman (DH) Key Exchange is one of the more popular and interesting methods of key distribution. It is a public-key cryptographic system whose sole purpose is for distributing keys. By the Diffie-Hellman key method the source's to use the separate keys for the each user in network, using these key the source node will transmit the data for destination. The key distribution to sensor nodes is done by means of two layer process. This paper proposes a key distribution scheme, based on intrusion detection method for using a data transmission from source to destination on the network. It based high level security on their network.*

Keywords: *Mobile Ad hoc Network (MANET); Intrusion Detection System; Diffie –Hellman (DH)*

I. INTRODUCTION

The Mobile ad hoc networks (MANETs) have attracted a lot of attentions due to their interesting and promising functionalities including mobile safety, traffic congestion avoidance, and location based services. In this paper, we focus on safety driving application, where each vehicle periodically broadcasts messages including its current position, direction and velocity, as well as road information. Privacy is an important issue in MANETs. As the wireless communication channel is a shared medium, exchanging messages without any security protection over the air can easily leak the information that users may want to keep private. Pseudonym based schemes have been proposed to preserve the location privacy of mobile. However, those schemes require the mobile to store a large number of pseudonyms and certifications, and do not support some important secure functionality such as authentication and integrity.

Rapid development in silicon technology is enabling the chips to accommodate billions of transistors. It has been observed however, that the current on-chip interconnect are becoming a bottleneck as they are unable to cope with growing number of participating cores on a chip. This inability of buses has convinced designers to look beyond their current domain and explore parallel architectures and computer networks. This has yielded a novel and scalable design for future interconnects for System on Chips termed as Network on Chips. This new communication paradigm for introduces the idea of creating a network of resources on a chip where communication takes place by routing packets between the resources instead of connecting them with dedicated. Such a structure will be supported by a set of protocols which provides well defined interfaces in order to separate communication from computation. As the size of a chip increases, so does the importance of error detection and recovery ('self-healing'); thus, it seems that the reliability of on-chip communication should be a primary issue.

Our protocol works under the assumption of mobile nodes which collaboratively support network operation. Network partitions can occur at any time and membership can change frequently. We define as group the set of nodes which can communicate through routes of one or more hops. Nodes in the same group must share the same group key to exchange routing control messages. We suppose that nodes run secure optimized link state routing protocol, a link state proactive routing protocol. Then, all nodes always know the number of nodes with which they can communicate. Besides, secure optimized link state routing protocol controls flooding with a mechanism called Multipoint Relays. In this mechanism, only nodes selected as MPR forward control messages. MPR nodes are selected by each node amongst the set of one hop neighbors, in a way to reach all two-hop neighbors. Also, nodes discover the approximately delay between its clocks in secure optimized link state routing protocol to avoid replay attacks. This information is used in our proposal to establish a weak synchronization on the network.

II. RELATED WORK

The risk aware response system [1] enhanced with the nodes can be selected the path with the important factors Evidence collection, risk assessment, decision making. With the changes of Routing Table Change Detector, nodes can be evaluated. The nodes can be achieved in the path with the risk evaluation. Dempster – Shafer theory can be used for evidence notations. The path can be set with static approach in Dempster –Shafer theory along with the network.

Secure Access for MANET Using Authorization Enforcement Facility [2] enhanced with the nodes security with Intrusion Detection system and the path can be selected the path with the dynamic access control. By the dynamic access control security can be provided to the network .And the networks can be selected with the various elements such as nodes and services, node value and service value, roles of the node value and the service value, thresholds, threat level and its action. This paper concentrated in the Intrusion Detection system and dynamic policy changes.

III. PROBLEM DESCRIPTION

In proposed system the Diffie-Hellman key exchange is vulnerable to attacks whereby an intruder intercepts messages between the sender and receiver, and assumes the identity of the other party. Consequently, the Diffie-Hellman algorithm should be used with a form of authentication such as certificates to ensure that symmetric keys are established between legitimate parties. The data send from source to destination on network through a base station. That time have any attacker to attack the data, so implement to avoid that data loss on network, using the secret key is generated for an each node; it has secure and more flexible on the network. The parameters for throughput, delay and energy level using to better results on the network. To Increase the network performance means using the two ways, there are static and dynamic path. Static means to use the same path for all the sources, then dynamic means all sources used the separate path for the network By using the Diffie Hellman scheme in the network, can solve the anonymous problem. Diffie Hellman scheme MAC address can be secured by that nodes can be secured. For the network performance path can be reset with static and dynamic ways.

By the Fig 3.1 static network, path can be set with node 0 can send data can pass the data by node 1 or by node 2. It passes the data to the node 4 or node 5 by using node 3to the destination node 6 of the network.

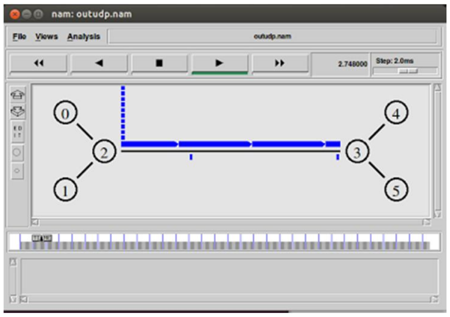

Fig 3.1 Static network

By the Fig 3.2 dynamic network, path can be set with node 0 can send data either by using node 1 or node 2 pass with use of node 4 or node 5 to the destination node.

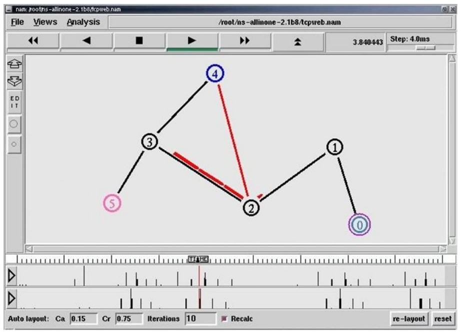
Auto layout: Ca 0.15 Cr 0.75 Iterations 10 Recalc
nam: /root/ns-allinone-2.1b8/tcpweb.nam
File
Views
Analysis
/root/ns-allinone-2.1b8/tcpweb.nam
3.840443
Step: 4.0ms
4
3
1
5
2
0
TIME
re-layout
reset

Fig 3.2

Dynamic network

The network performance increment by setting the path with neither static nor dynamic. By the bandwidth efficiency node can be select for network transmission. Transmission can be done with efficient way with node setting with the Diffie Hellman scheme. By the Fig 3.3 can be get the clear understanding graph can be plotted with the bandwidth and latency method.

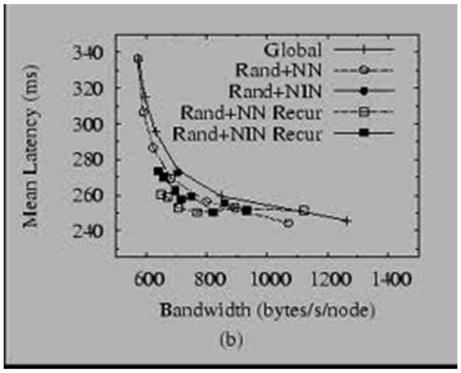

Fig 3.3 Static and Dynamic network

The Steps can be involved for the Diffie-Hellman with the network design with static and dynamic path.

Step 1:

The source nodes have the every node key and his address.

Step 2:

If source node wish to send data. To check the neighbors' node has key means to transfer the data in that node. Else, thus not send data**,** again to check the key

Step 3:

The node is to collect the information and key.

Step 4:

To checking the all node key, finally to send data means the key will be automatically exchange.

Step 5:

Using this key the data will be sending in efficient manner as well as without any loss data.

IV. MODULES DESCRIPTION

1. Wireless Network Configure Setting

Wireless Networks to create the no of nodes. The packets to send and receiving through the source to destination. It's based the scheme of packets delivered for ACK packet drop on the nodes. In this network to creating the source and destination node of the network and transmit the data to processing on their whole networking.

2. Topology Design

This module is developed to Topology design all node place particular distance. Without using any cables then fully wireless sensor equipment based transmission and received packet data. Node and wireless between calculate sending and receiving packets. The cluster head is at the center of the circular sensing area. Intermediate the sender and receiver of this networking performance on this topology.

3. Node Creating

This module is developed to node creation and more than 10 nodes placed particular distance. Wireless node placed intermediate area. Each node knows its location relative to the sink. The access point has to receive transmit packets then send acknowledge to transmitter.

4. Collusion Attack

Due to the dynamic nature of the clustering formation in the Manet the sensor nodes are collide with the key generation node and thus lead to the security issue, as soon as collusion takes place the cluster head selects another KG node and keying process continues.

5. Diffie-Hellman Algorithm

It should be complemented with an authentication mechanism. In this approach for key distribution in security factors with respect fact that solving attacking problem is very challenging and that the shared key is never itself transmitted over the channel.

V. CONCULSION

The Intrusion Detection System using the Diffie Hellman key exchange method used to be one of the most interesting key distribution schemes in use today. However, one must be aware of the fact that although the algorithm is safe against passive eaves dropping, it is not necessarily protected from active attacks distribution to allow malicious nodes to interact within the network for transferring data between sources to destination and hence complete security could not be achieved within the network due to the presence of malicious nodes. In order to provide more secure communication between source and destination, DH uses risk as an input to determine how much source node can be trusted, so that only trusted nodes are allowed to communicate and hence high security can be achieved within MANET. This paper enhances to take a throughput, delay and delivery ratio are network performance on the network. It most efficient and security based data transmission.

REFERENCES

[1] Risk-Aware Mitigation for MANET Routing Attacks, Risk-Aware Mitigation for MANET Routing Attacks, IEEE, VOL. 9, NO. 2, MARCH/APRIL 2012.

[2] Secure Access for MANET Using Authorization Enforcement Facility, Gowthami, Sangeetha, ICICES, 2013.

[3] Mohammed N., Otrok H. Wang L. Debbabi M. and Bhattacharya P., 'Mechanism Design-Based Secure Leader Election Model for Intrusion Detection in MANET' IEEE Transaction, Dependable and Secure Computing, Vol. 8, pp. 89-103, 2011.

[4] Marti S., Giuli T. Lai K. and Baker M.,'Mitigating Routing Misbehavior in Mobile Ad Hoc Networks', Proceedings of ACM Mobile Communication, pp. 255-265,2000

[5] Refaei M., DaSilva L. Eltoweissy M. and Nadeem T.,'Adaptation of Reputation Management Systems to Dynamic Network Conditions in AdHoc Networks', vol. 59,pp. 707-719, 2010.

[6] Teo L., Ahn G. and Zheng Y., 'Dynamic and Risk – Aware Network Access Management', Proceedings of Eighth ACM Symposium, Access Control Models a Technologies, pp. 217-230, 2003.

[7] Tseng C., Wang S. Ko C. and Levitt K.,'DEMEM: Distribute Evidence Driven Message Exchange Intrusion Detection Model For Manet Proceedings on 9th international Symposium, Recent Advances in Intrusion Detection, pp. 249-271, 2006.